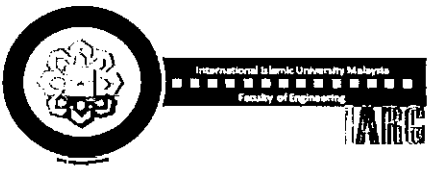
Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM PRESS
2011



Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM Press
2011

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

Perpustakaan Negara Malaysia Cataloguing-in-Publication Data

Mohammad Umar Siddiqi, Sigit Puspito Wigati Jarot and Othman Omran Khalifa: Topics in Coding, Cryptography and Information Security

ISBN: 978-967-418-169-7

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

Topics in Coding, Cryptography and Information Security

Contents

List of Contributors ii

Editorial Introduction vi

PART I: SOURCE CODING

1. Performance Analysis of Image Data Compression using Zero-Tree Wavelet Transform 2
   Othman O. Khalifa, Emir Tabakovic, Zlatko Memisevic and Aisha-Hassan Abdullah

2. Scalable and Robust Streaming Video System Challenges 12
   Othman O. Khalifa, Sinzobakwira Issa and Mohammad Umar Siddiqi

PART II: CHANNEL CODING

3. Golay Codec: An Overview 23
   Othman O. Khalifa

4. Reed-Muller Codes: An Overview 35
   Othman O. Khalifa

5. Viterbi Decoder: A Review and Implementation 42
   Noorainani Ainina Bt. Md Noor Albakri and Othman O. Khalifa

6. Zigzag Codes: High Rate Low Complexity Iterative Codes 53
Sigit P.W. Jarot

7. Convolutional Coded OFDM in Broadband Mobile Communication 66
Sigit P.W. Jarot

8. Channel Coding Techniques in Mobile Communication Systems 77
Othman O. Khalifa and Rashid A. Saeed

9. Channel Coding in CDMA 2000 85
Othman O. Khalifa

10. Channel Coding in Mobile WiMAX 91
Rashid A. Saeed and Othman O. Khalifa

11. Turbo Codes: An Error Correction Technique for 4G 99
Mosharrof Hussain Masud and Mohammad Umar Siddiqi

12. Combined Source Channel Decoding for Image Transmission over Noisy Channels 108
Jalel Chebil

PART III: CRYPTOGRAPHY AND INFORMATION SECURITY

13. Cryptographic Boolean Functions: Transform Domain Perspective 120
Hashum Mohamed Rafiq and Mohammad Umar Siddiqi

14. Implementation of RSA Algorithm 141
Hafizul Azizi Rasid, Mohd Azmi Jabar and Othman O. Khalifa

15. GSM Security: Problems and Solutions 152
Rashid A. Saeed and Othman O. Khalifa

16. Recent Approaches to Wireless Physical Layer Security 161
M. Tahir, Sigit P.W. Jarot and M.U. Siddiqi

17. Securing OFDM-based Systems from the Physical Layer 169
Sigit P.W. Jarot

18. Simulation of Artificial Noise based Physical Layer Security 174
Muhammad Izzat bin Zurkiple and Sigit Puspito Wigati Jarot

19. Secure IPv6 Address Generation 183
Nashrul Hakiem, Mohammad Umar Siddiqi, and Sigit Puspito Wigati Jarot

20. Video Streaming and Encrypting Algorithms 190
Mohammed Abumuala, Othman O. Khalifa, and Aisha-Hassan A. Hashim

21. Wireless IP Camera based on Motion Detection Surveillance System 217
Zeeshan Shahid and Khaizuran Abdullah

22. Design of Mobile Phone Jammer 223
Fauzun Abdullah Asuhaimi, Nur Fatin Mohd Zakki, and Khaizuran Abdullah

Index

Chapter 2

Scalable and Robust Streaming Video System Challenges

Othman O. Khalifa, Sinzobakwira Issa and Mohammad Umar Siddiqi

2.1. Introduction

The development of multimedia propagations and applications has led to a greater demand in the field of video transmission over a heterogeneous media as well as iterative delivery platforms with dedicated content requirements. In general, there are two approaches to provide multimedia services on demand: *offline downloading* and *online streaming*. Since the streaming approach enables users to experience a multimedia presentation on the fly while it is being downloaded from the Internet, it has prevailed in both the academia and the industry. In virtue of the streaming techniques, users no longer have to suffer from long and even unacceptable transport time for full download. It is known that conventional video coding systems encode video content with given bitrates adapted to a specific function or application. As a result, conventional video coding does not meet the fundamental requirements of the state-of-the-art flexible digital media application. For video encoding, there are two ways to compress the video signals: non-scalable video coding and scalable video coding. In non-scalable video coding, the video content is encoded independent of actual channel characteristics. In this method, coding efficiency is the most important factor and the compression is optimized at a pre-specified rate. The main problem with this method is that it is difficult to adaptively stream non-scalable video contents to heterogeneous client terminals over time-varying communication channels [1]. .Figure 2.1 shows a typical stream for video system. This streaming system consists of nth input video, encoder, a distribution server to store videos, a relay server and several end-users receiving video data.